ID: 404248
Sample Name: invoice.exe
Cookbook: default.jbs
Time: 20:46:16
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

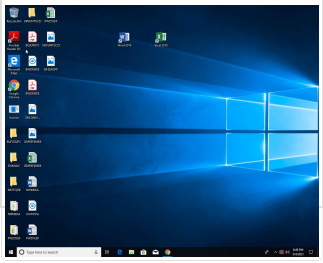
Analysis Report invoice.exe

Overview

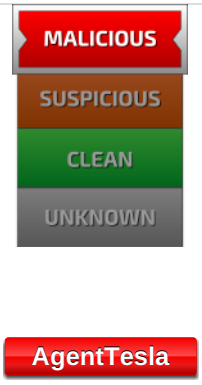
General Information

Sample Name:	invoice.exe
Analysis ID:	404248
MD5:	1a59efb27c11d1a.
SHA1:	6c5513edcdbbec..
SHA256:	35a971b8e884d2..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



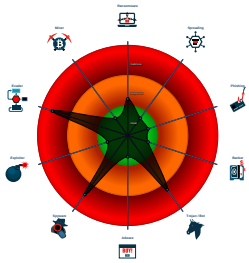
AgentTesla

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…

Classification



Startup

- **System is w10x64**
- invoice.exe (PID: 6980 cmdline: 'C:\Users\user\Desktop\invoice.exe' MD5: 1A59EFB27C11D1AE0959BF6661E23538)
  - invoice.exe (PID: 6488 cmdline: C:\Users\user\Desktop\invoice.exe MD5: 1A59EFB27C11D1AE0959BF6661E23538)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "kxguy@chefoowork.comVttn8SluiOogmail.chefoowork.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.669341704.00000000032C2000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000002.913638464.0000000002EB1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.913638464.0000000002EB1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.670894722.0000000004259000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.910976432.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 4 entries

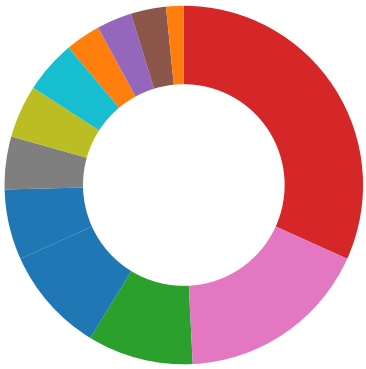
Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.invoice.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.invoice.exe.435f638.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.invoice.exe.435f638.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:

Initial sample is a PE file and has a suspicious name

Malware Analysis System Evasion:

Yara detected AntiVM3

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

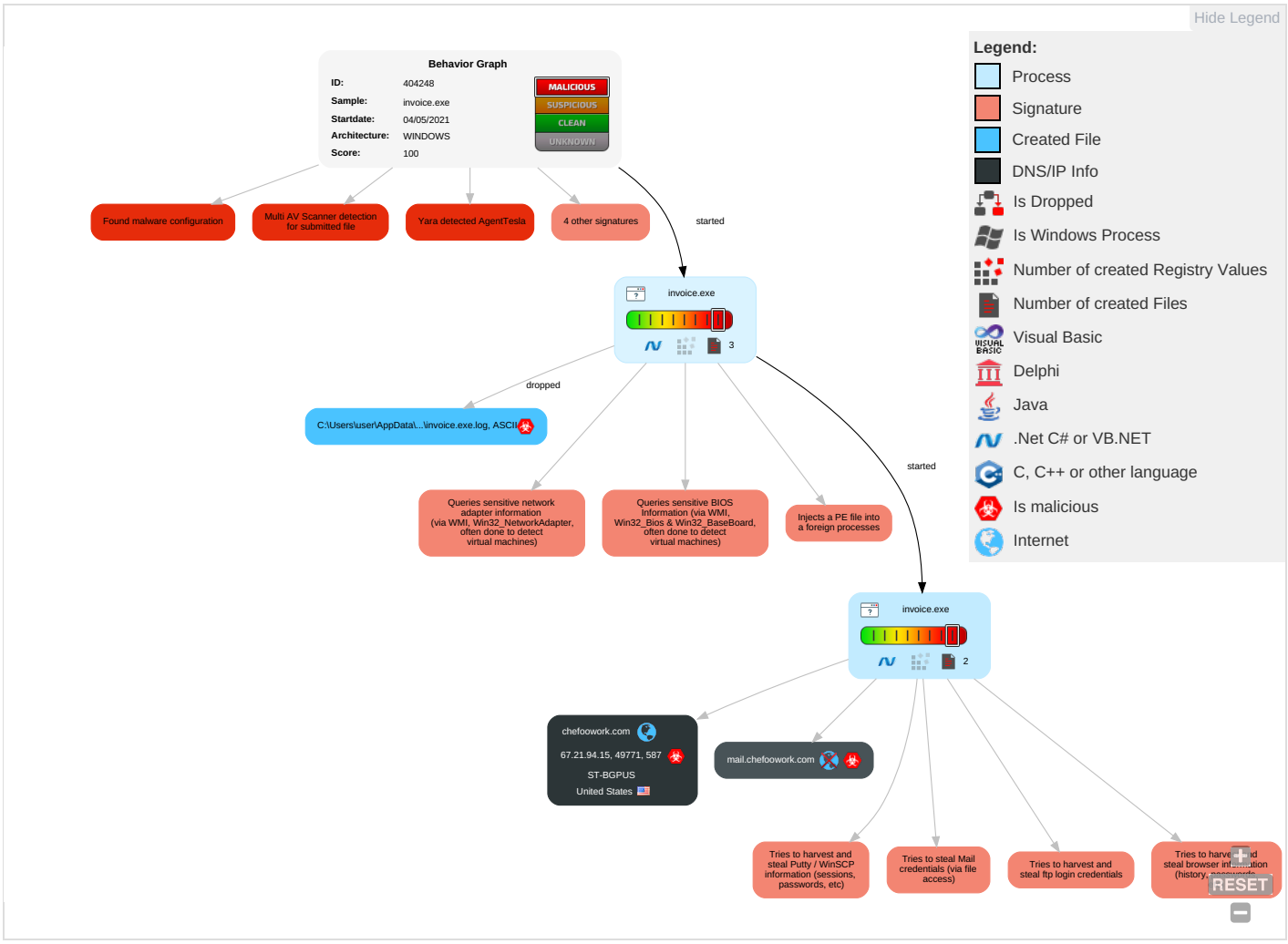
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Credentials in Registry 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 3	Cached Domain Credentials	Account Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 1 1 4	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocol

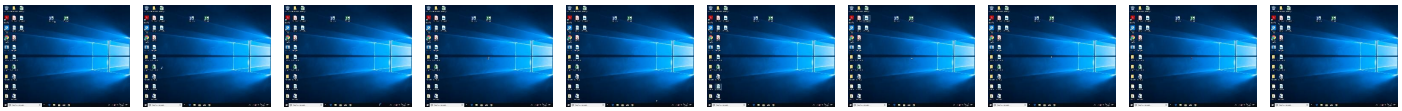
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
invoice.exe	17%	ReversingLabs	ByteCode-MSIL.Packed.Generic	
invoice.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.invoice.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
chefoowork.com	0%	Virustotal		Browse
mail.chefoowork.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.tiro.com:	0%	Virustotal		Browse
http://www.tiro.com:	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr-i	0%	Avira URL Cloud	safe	
http://www.fontbureau.commva	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://XMBduf.com	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://chefoowork.com	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fonts.comnO	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.churchsw.org/church-projector-project	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.krH	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.sandoll.co.krormal	0%	Avira URL Cloud	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://ynmdZVkfPM0WUw.com	0%	Avira URL Cloud	safe	
http://www.fonts.comic3	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cno.4k	0%	Avira URL Cloud	safe	
http://www.churchsw.org/repository/Bibles/	0%	Avira URL Cloud	safe	
http://mail.chefoowork.com	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krN.TTF	0%	Avira URL Cloud	safe	
http://www.goodfont.co.krF	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htmWl	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comtl	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.sakkal.com-e	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
chefoowork.com	67.21.94.15	true	true	• 0%, Virustotal, Browse	unknown
mail.chefoowork.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

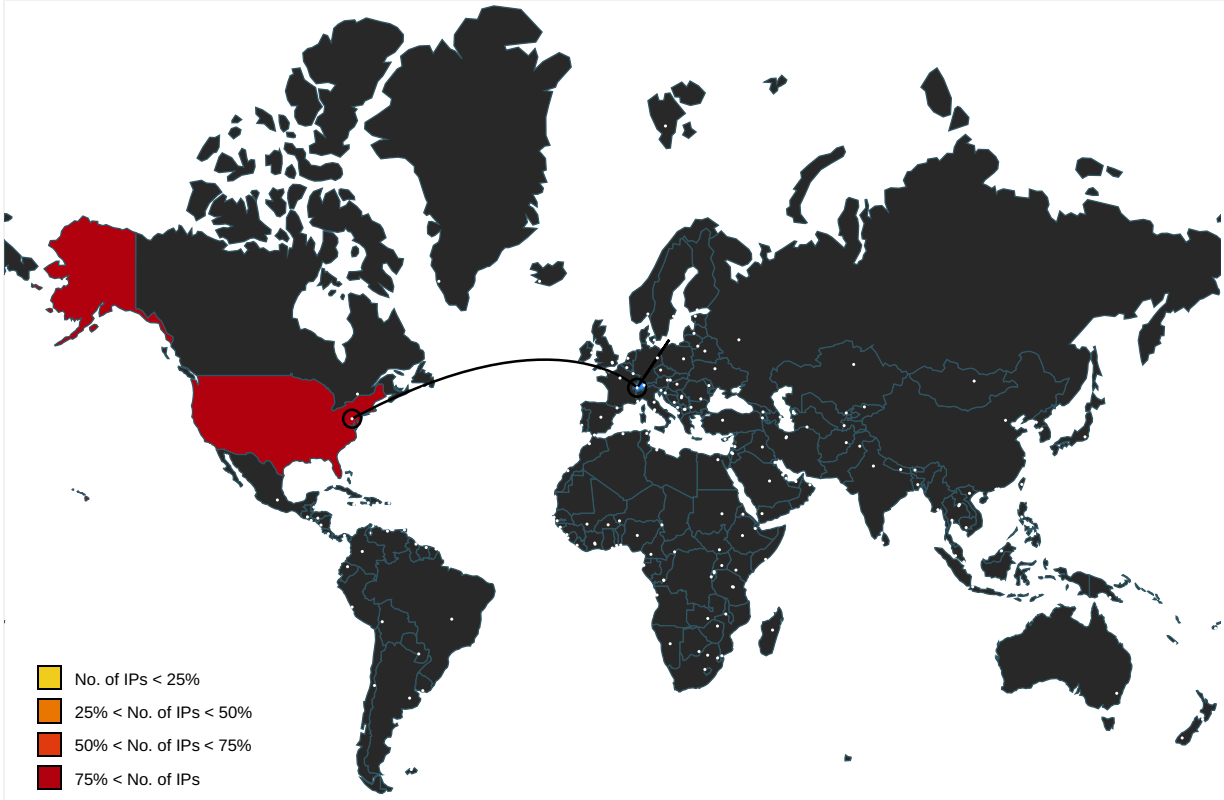
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com:	invoice.exe, 00000000.00000003.645972306.000000000648B000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	invoice.exe, 00000004.00000002.913638464.0000000002EB1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr-i	invoice.exe, 00000000.00000003.646701127.0000000006480000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.commva	invoice.exe, 00000000.00000002.669124554.0000000001910000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://XMBduf.com	invoice.exe, 00000004.00000002.913638464.0000000002EB1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false		high
http://www.tiro.com	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://chefoowork.com	invoice.exe, 00000004.00000002.914437799.0000000003214000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	invoice.exe, 00000000.00000002.669341704.00000000032C2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/G	invoice.exe, 00000000.00000003.649460358.000000000647C000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	invoice.exe, 00000000.00000003.652670720.000000000647C000.00000004.00000001.sdmp, invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comgrita	invoice.exe, 00000000.00000002.669124554.0000000001910000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comnO	invoice.exe, 00000000.00000003.645760203.000000000648B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	invoice.exe, 00000000.00000003.648358482.000000000647C000.00000004.00000001.sdmp, invoice.exe, 00000000.00000003.648325032.000000000647C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.churchsw.org/church-projector-project	invoice.exe	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	invoice.exe, 00000000.00000003.645807019.000000000648B000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krH	invoice.exe, 00000000.00000003.646701127.0000000006480000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krormal	invoice.exe, 00000000.00000003.646701127.0000000006480000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.de	invoice.exe, 00000000.00000003.651230932.000000000647C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	invoice.exe, 00000000.00000002.669242244.0000000003251000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	invoice.exe, 00000000.00000002.670894722.0000000004259000.00000004.00000001.sdmp, invoice.exe, 00000004.00000002.910976432.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	invoice.exe, 00000004.00000002.913638464.0000000002EB1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	invoice.exe, 00000004.00000002.912327944.000000000117B000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	invoice.exe, 00000004.00000002.913638464.0000000002EB1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ynmdZVkfPM0WUw.com	invoice.exe, 00000004.00000002.913638464.0000000002EB1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comic3	invoice.exe, 00000000.00000003.645760203.000000000648B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cno.4k	invoice.exe, 00000000.00000003.647562258.0000000006473000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers/cabarga.htmlx	invoice.exe, 00000000.00000003.650651642.000000000647C000.00000004.00000001.sdmp	false		high
http://www.churchsw.org/repository/Bibles/	invoice.exe	false	• Avira URL Cloud: safe	unknown
http://mail.chefoowork.com	invoice.exe, 00000004.00000002.914437799.0000000003214000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krN.TTF	invoice.exe, 00000000.00000003.646701127.0000000006480000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.krF	invoice.exe, 00000000.00000003.646701127.0000000006480000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	invoice.exe, 00000000.00000003.647422674.0000000006473000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/staff/dennis.htmWl	invoice.exe, 00000000.00000003.652670720.000000000647C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	invoice.exe, 00000000.00000003.650506259.0000000006484000.00000004.00000001.sdmp, invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	invoice.exe, 00000000.00000003.650618133.000000000647C000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comtl	invoice.exe, 00000000.00000002.669124554.0000000001910000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers8	invoice.exe, 00000000.00000002.677620808.0000000007702000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/frere-user.htmlx	invoice.exe, 00000000.00000003.650173899.000000000647C000.00000004.00000001.sdmp	false		high
http://www.sakkal.com-e	invoice.exe, 00000000.00000003.648325032.000000000647C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
67.21.94.15	chefoowork.com	United States		46844	ST-BGPUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404248
Start date:	04.05.2021
Start time:	20:46:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	invoice.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0

Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@2/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 13.64.90.137, 52.147.198.201, 2.20.157.220, 168.61.161.212, 20.50.102.62, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129, 2.20.142.209, 2.20.142.210, 20.49.157.6 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:47:12	API Interceptor	749x Sleep call for process: invoice.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
67.21.94.15	ATuRNgegI7kl7Ua.exe	Get hash	malicious	Browse	
	Vcv22W33OiwhO12.exe	Get hash	malicious	Browse	
	Catalog.exe	Get hash	malicious	Browse	
	5401628864_AWB_28002_2021-17-03 2.exe	Get hash	malicious	Browse	
	AVISO CREDITO PAGPROV.exe	Get hash	malicious	Browse	
	7070355.exe	Get hash	malicious	Browse	
	OC_402981675.exe	Get hash	malicious	Browse	
	OC_007943234.exe	Get hash	malicious	Browse	
	QIznD4DaCkKgV4J.exe	Get hash	malicious	Browse	
	U6ODBh62dJ0lYCK.exe	Get hash	malicious	Browse	
	OC_8403754263563.exe	Get hash	malicious	Browse	
	jc7xI20UOg.exe	Get hash	malicious	Browse	
	xIpnl7dBEb.exe	Get hash	malicious	Browse	
	rm1E9ZjuNd.exe	Get hash	malicious	Browse	
	DHL Shipment Info.exe	Get hash	malicious	Browse	
	RFQ.4414_122.exe	Get hash	malicious	Browse	
	GimRyEHi4ONqTEe.exe	Get hash	malicious	Browse	
	PO_2002837727_288772.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ST-BGPUS	ATuRNgegI7kl7Ua.exe	Get hash	malicious	Browse	• 67.21.94.15
	Vcv22W33OiwhO12.exe	Get hash	malicious	Browse	• 67.21.94.15
	Catalog.exe	Get hash	malicious	Browse	• 67.21.94.15
	SecuriteInfo.com.Trojan.DownloaderNET.160.29545.exe	Get hash	malicious	Browse	• 67.21.94.4
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 204.188.203.155
	RCS76393.exe	Get hash	malicious	Browse	• 104.160.174.177
	eQLPRPErea.exe	Get hash	malicious	Browse	• 64.32.22.102
	UTcQK0heAfGWTLw.exe	Get hash	malicious	Browse	• 64.32.22.102
	RFQ # 1014397402856.pdf.exe	Get hash	malicious	Browse	• 204.188.203.155
	BIOTECHPO960488580.exe	Get hash	malicious	Browse	• 205.144.171.210
	GJK-KAOHSIUNG-2101.xlsx	Get hash	malicious	Browse	• 205.144.171.138
	New Purchase Order.exe	Get hash	malicious	Browse	• 204.188.203.155
	9311-32400.pdf.exe	Get hash	malicious	Browse	• 45.58.190.82
	ssyrNaO6AP.dll	Get hash	malicious	Browse	• 70.39.99.196
	5401628864_AWB_28002_2021-17-03 2.exe	Get hash	malicious	Browse	• 67.21.94.15
	SPmG3TLdax.exe	Get hash	malicious	Browse	• 204.188.203.155
	RDAW-180-47D.exe	Get hash	malicious	Browse	• 64.32.22.102
	Doc_3847468364836483638463,pdf.exe	Get hash	malicious	Browse	• 170.178.168.203
	gV8xdP8bas.exe	Get hash	malicious	Browse	• 104.160.174.169
	DHL.INFORMATION.TRACKING.exe	Get hash	malicious	Browse	• 67.21.94.4

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\invoice.exe.log	
Process:	C:\Users\user\Desktop\invoice.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.612907586857075
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	invoice.exe
File size:	657408
MD5:	1a59efb27c11d1ae0959bf6661e23538
SHA1:	6c5513edcdbbec2e332601bc136c3bf293b257fd
SHA256:	35a971b8e884d2d443a0d998e1f5c86cac85fe32af0eac3ba3bd518580f26678
SHA512:	7edebf42e9c80b7de2b6e31bf6d997ac7bcb3b64aff48119a6eb6287cb43f3b810dd80238f39c1b83d64ab4dfce6bf9757b349d9255a890c06eeb588dc6b3cc8
SSDEEP:	12288:NGgJvG5+IQEOKMrkXAEcapHnZWa7lDrGeZ7J3UvnjK:MgJvDTEOKNXFpEA7Jk
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....b.... ... ....@.. .....`.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4a1d62
Entrypoint Section:	.text

General

Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60912EF9 [Tue May 4 11:24:41 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa1d10	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa2000	0x424	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa4000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x9fd68	0x9fe00	False	0.795957229769	data	7.62508857658	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa2000	0x424	0x600	False	0.289713541667	data	2.42756322043	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa4000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xa2058	0x3c8	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Felix Jeyareuben 2012
Assembly Version	2.0.0.0
InternalName	RijndaelManagedTransform.exe
FileVersion	2.0
CompanyName	www.churchsw.org
LegalTrademarks	Church Software
Comments	
ProductName	Church Projector
ProductVersion	2.0
FileDescription	Church Projector
OriginalFilename	RijndaelManagedTransform.exe

Network Behavior

Network Port Distribution

Total Packets: 61

- 53 (DNS)
- 587 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:48:55.886637926 CEST	49771	587	192.168.2.4	67.21.94.15
May 4, 2021 20:48:56.079209089 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:56.079359055 CEST	49771	587	192.168.2.4	67.21.94.15
May 4, 2021 20:48:56.438600063 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:56.439112902 CEST	49771	587	192.168.2.4	67.21.94.15
May 4, 2021 20:48:56.631918907 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:56.632364988 CEST	49771	587	192.168.2.4	67.21.94.15
May 4, 2021 20:48:56.827056885 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:56.874015093 CEST	49771	587	192.168.2.4	67.21.94.15
May 4, 2021 20:48:56.903604984 CEST	49771	587	192.168.2.4	67.21.94.15
May 4, 2021 20:48:57.106219053 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:57.106261969 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:57.106272936 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:57.106292963 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:57.106308937 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:57.106417894 CEST	49771	587	192.168.2.4	67.21.94.15
May 4, 2021 20:48:57.106499910 CEST	49771	587	192.168.2.4	67.21.94.15
May 4, 2021 20:48:57.111130953 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:57.148775101 CEST	49771	587	192.168.2.4	67.21.94.15
May 4, 2021 20:48:57.342194080 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:57.389724016 CEST	49771	587	192.168.2.4	67.21.94.15
May 4, 2021 20:48:57.683432102 CEST	49771	587	192.168.2.4	67.21.94.15
May 4, 2021 20:48:57.877511978 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:57.878709078 CEST	49771	587	192.168.2.4	67.21.94.15
May 4, 2021 20:48:58.071715117 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:58.072448015 CEST	49771	587	192.168.2.4	67.21.94.15
May 4, 2021 20:48:58.306613922 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:58.501542091 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:58.502100945 CEST	49771	587	192.168.2.4	67.21.94.15
May 4, 2021 20:48:58.693665028 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:58.694238901 CEST	49771	587	192.168.2.4	67.21.94.15
May 4, 2021 20:48:58.925160885 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:58.925677061 CEST	49771	587	192.168.2.4	67.21.94.15
May 4, 2021 20:48:59.117305994 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:59.119545937 CEST	49771	587	192.168.2.4	67.21.94.15
May 4, 2021 20:48:59.119587898 CEST	49771	587	192.168.2.4	67.21.94.15
May 4, 2021 20:48:59.119761944 CEST	49771	587	192.168.2.4	67.21.94.15
May 4, 2021 20:48:59.119770050 CEST	49771	587	192.168.2.4	67.21.94.15
May 4, 2021 20:48:59.313139915 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:59.313165903 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:59.313178062 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:59.313189030 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:59.319694996 CEST	587	49771	67.21.94.15	192.168.2.4
May 4, 2021 20:48:59.374453068 CEST	49771	587	192.168.2.4	67.21.94.15

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:46:55.308562040 CEST	49714	53	192.168.2.4	8.8.8.8
May 4, 2021 20:46:55.357300997 CEST	53	49714	8.8.8.8	192.168.2.4
May 4, 2021 20:46:56.418832064 CEST	58028	53	192.168.2.4	8.8.8.8
May 4, 2021 20:46:56.478195906 CEST	53	58028	8.8.8.8	192.168.2.4
May 4, 2021 20:46:57.204322100 CEST	53097	53	192.168.2.4	8.8.8.8
May 4, 2021 20:46:57.261778116 CEST	53	53097	8.8.8.8	192.168.2.4
May 4, 2021 20:46:57.664890051 CEST	49257	53	192.168.2.4	8.8.8.8
May 4, 2021 20:46:57.733747005 CEST	53	49257	8.8.8.8	192.168.2.4
May 4, 2021 20:46:58.863512039 CEST	62389	53	192.168.2.4	8.8.8.8
May 4, 2021 20:46:58.913793087 CEST	53	62389	8.8.8.8	192.168.2.4
May 4, 2021 20:47:00.198642969 CEST	49910	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:00.250102997 CEST	53	49910	8.8.8.8	192.168.2.4
May 4, 2021 20:47:01.562326908 CEST	55854	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:01.614088058 CEST	53	55854	8.8.8.8	192.168.2.4
May 4, 2021 20:47:02.595196962 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:02.643806934 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 20:47:03.724561930 CEST	63153	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:03.773454905 CEST	53	63153	8.8.8.8	192.168.2.4
May 4, 2021 20:47:04.540361881 CEST	52991	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:04.591876984 CEST	53	52991	8.8.8.8	192.168.2.4
May 4, 2021 20:47:05.475644112 CEST	53700	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:05.534707069 CEST	53	53700	8.8.8.8	192.168.2.4
May 4, 2021 20:47:06.600827932 CEST	51726	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:06.663393974 CEST	53	51726	8.8.8.8	192.168.2.4
May 4, 2021 20:47:07.509717941 CEST	56794	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:07.558408022 CEST	53	56794	8.8.8.8	192.168.2.4
May 4, 2021 20:47:08.445209026 CEST	56534	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:08.493815899 CEST	53	56534	8.8.8.8	192.168.2.4
May 4, 2021 20:47:09.325426102 CEST	56627	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:09.376822948 CEST	53	56627	8.8.8.8	192.168.2.4
May 4, 2021 20:47:10.308964968 CEST	56621	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:10.357498884 CEST	53	56621	8.8.8.8	192.168.2.4
May 4, 2021 20:47:11.503861904 CEST	63116	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:11.554511070 CEST	53	63116	8.8.8.8	192.168.2.4
May 4, 2021 20:47:12.633982897 CEST	64078	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:12.682523966 CEST	53	64078	8.8.8.8	192.168.2.4
May 4, 2021 20:47:13.799525023 CEST	64801	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:13.849663019 CEST	53	64801	8.8.8.8	192.168.2.4
May 4, 2021 20:47:27.419760942 CEST	61721	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:27.469161034 CEST	53	61721	8.8.8.8	192.168.2.4
May 4, 2021 20:47:31.472867966 CEST	51255	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:31.535389900 CEST	53	51255	8.8.8.8	192.168.2.4
May 4, 2021 20:47:45.299133062 CEST	61522	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:45.420372009 CEST	53	61522	8.8.8.8	192.168.2.4
May 4, 2021 20:47:46.005215883 CEST	52337	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:46.302139997 CEST	53	52337	8.8.8.8	192.168.2.4
May 4, 2021 20:47:46.897455931 CEST	55046	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:46.954340935 CEST	53	55046	8.8.8.8	192.168.2.4
May 4, 2021 20:47:47.068720102 CEST	49612	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:47.126574039 CEST	53	49612	8.8.8.8	192.168.2.4
May 4, 2021 20:47:47.382806063 CEST	49285	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:47.592140913 CEST	53	49285	8.8.8.8	192.168.2.4
May 4, 2021 20:47:48.278194904 CEST	50601	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:48.330339909 CEST	53	50601	8.8.8.8	192.168.2.4
May 4, 2021 20:47:48.970706940 CEST	60875	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:49.030683041 CEST	53	60875	8.8.8.8	192.168.2.4
May 4, 2021 20:47:49.419503927 CEST	56448	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:49.479090929 CEST	53	56448	8.8.8.8	192.168.2.4
May 4, 2021 20:47:49.534406900 CEST	59172	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:49.591427088 CEST	53	59172	8.8.8.8	192.168.2.4
May 4, 2021 20:47:50.654434919 CEST	62420	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:50.713545084 CEST	53	62420	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:47:51.629568100 CEST	60579	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:51.678473949 CEST	53	60579	8.8.8.8	192.168.2.4
May 4, 2021 20:47:52.210251093 CEST	50183	53	192.168.2.4	8.8.8.8
May 4, 2021 20:47:52.261642933 CEST	53	50183	8.8.8.8	192.168.2.4
May 4, 2021 20:48:01.715611935 CEST	61531	53	192.168.2.4	8.8.8.8
May 4, 2021 20:48:01.772701979 CEST	53	61531	8.8.8.8	192.168.2.4
May 4, 2021 20:48:02.103682041 CEST	49228	53	192.168.2.4	8.8.8.8
May 4, 2021 20:48:02.162940025 CEST	53	49228	8.8.8.8	192.168.2.4
May 4, 2021 20:48:05.248570919 CEST	59794	53	192.168.2.4	8.8.8.8
May 4, 2021 20:48:05.307259083 CEST	53	59794	8.8.8.8	192.168.2.4
May 4, 2021 20:48:36.449769020 CEST	55916	53	192.168.2.4	8.8.8.8
May 4, 2021 20:48:36.499744892 CEST	53	55916	8.8.8.8	192.168.2.4
May 4, 2021 20:48:38.232959986 CEST	52752	53	192.168.2.4	8.8.8.8
May 4, 2021 20:48:38.292238951 CEST	53	52752	8.8.8.8	192.168.2.4
May 4, 2021 20:48:55.333537102 CEST	60542	53	192.168.2.4	8.8.8.8
May 4, 2021 20:48:55.543627024 CEST	53	60542	8.8.8.8	192.168.2.4
May 4, 2021 20:48:55.554277897 CEST	60689	53	192.168.2.4	8.8.8.8
May 4, 2021 20:48:55.766128063 CEST	53	60689	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 20:48:55.333537102 CEST	192.168.2.4	8.8.8.8	0xa05b	Standard query (0)	mail.chefoowork.com	A (IP address)	IN (0x0001)
May 4, 2021 20:48:55.554277897 CEST	192.168.2.4	8.8.8.8	0xb24e	Standard query (0)	mail.chefoowork.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 20:48:55.543627024 CEST	8.8.8.8	192.168.2.4	0xa05b	No error (0)	mail.chefoowork.com	chefoowork.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 20:48:55.543627024 CEST	8.8.8.8	192.168.2.4	0xa05b	No error (0)	chefoowork.com		67.21.94.15	A (IP address)	IN (0x0001)
May 4, 2021 20:48:55.766128063 CEST	8.8.8.8	192.168.2.4	0xb24e	No error (0)	mail.chefoowork.com	chefoowork.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 20:48:55.766128063 CEST	8.8.8.8	192.168.2.4	0xb24e	No error (0)	chefoowork.com		67.21.94.15	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 4, 2021 20:48:56.438600063 CEST	587	49771	67.21.94.15	192.168.2.4	220-web2.changeip.com ESMTP Exim 4.94 #2 Tue, 04 May 2021 14:48:55 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 4, 2021 20:48:56.439112902 CEST	49771	587	192.168.2.4	67.21.94.15	EHLO 123716
May 4, 2021 20:48:56.631918907 CEST	587	49771	67.21.94.15	192.168.2.4	250-web2.changeip.com Hello 123716 [84.17.52.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-X_PIPE_CONNECT 250-STARTTLS 250 HELP
May 4, 2021 20:48:56.632364988 CEST	49771	587	192.168.2.4	67.21.94.15	STARTTLS
May 4, 2021 20:48:56.827056885 CEST	587	49771	67.21.94.15	192.168.2.4	220 TLS go ahead

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: invoice.exe PID: 6980 Parent PID: 5960

General

Start time:	20:47:02
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\invoice.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\invoice.exe'
Imagebase:	0xe00000
File size:	657408 bytes
MD5 hash:	1A59EFB27C11D1AE0959BF6661E23538
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.669341704.00000000032C2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.670894722.0000000004259000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D0FCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D0FCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\invoice.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D40C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\invoice.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D40C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BF41B4F	ReadFile

Analysis Process: invoice.exe PID: 6488 Parent PID: 6980

General

Start time:	20:47:13
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\invoice.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\invoice.exe
Imagebase:	0xa80000
File size:	657408 bytes
MD5 hash:	1A59EFB27C11D1AE0959BF6661E23538
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.913638464.0000000002EB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.913638464.0000000002EB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.910976432.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D0FCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D0FCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BF41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BF41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BF41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BF41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6BF41B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\e5a203ba-96cb-4de8-a8ad-bc4d6d4b3366	unknown	4096	success or wait	1	6BF41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6BF41B4F	ReadFile

Disassembly

Code Analysis